



IN THE U.S. PATENT AND TRADEMARK OFFICE

Appl. No. : 10/627,117
Applicant : Peter Dam Neilsen, et al.
Filed : July 24, 2003
TC/AU : 2167 (confirmation no. 3924)
Examiner : Timblin, Robert M.

Docket No. : 857.0019.U1(US)

Title : A Method for Controlling Access Rights to Data Stored in a Hand
Portable Device and Hand Portable Device Having Access to Data

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Pre-Appeal Request for Review

This paper is in response to the final Office Action dated July 2, 2008 for the above-referenced US Patent Application, and is filed with the Applicant's Notice of Appeal.

Claims 2, 3, 5-9, 20, 23, 33-40, 46 and 52-60 stand finally rejected. A complete listing of claims may be seen in the Applicant's Amendment dated April 7, 2008. All independent claims are rejected under 35 USC 103(a) as obvious over US Pub 2002/0091700 (Steele).

Arguing only the independent claim 20 in this paper does not relinquish the Applicants' right to argue further claims on appeal to the Board. Claim 20 recites: A method comprising:

- a) storing a plurality of data assemblages in a hand portable device;
- b) storing at least one data attribute for each of the plurality of data assemblages, the data attribute indicative of first display of the data assemblage in the device;
- c) displaying for a first time in the hand portable device a first data assemblage of the plurality without regard to a first security mechanism, and responsive to the displaying for the first time automatically changing the data attribute of the first data assemblage from a first type to a second type; and
- d) in response to changing the data attribute of step c), automatically restricting further display of the first data assemblage using the first security mechanism.

Page 5 lines 1-10 of the application gives a non-limiting example for illustration. A mobile telephone receives an SMS message (element a). A data attribute (e.g., a bit) indicates that the SMS has not yet been displayed (element b). Displaying the SMS for the first time at the mobile telephone does not require a password since the data attribute indicates that it has not yet been displayed, but upon first display of the SMS at the mobile telephone the data attribute automatically changes (element c). Subsequent display of the SMS at the mobile telephone requires a password due to the changed data attribute (element d).

The sole reference against claim 20 is Steele, which teaches a database for creating and storing text and graphic/image content using a standard PC in which data is manipulated and thereafter loaded onto a PDA for viewing (abstract). ¶ [0009] describes a problem that relational databases consume substantial system resources which are extremely limited on handheld computers. The Steele solution is described at ¶ [0014] as having no need to update records on the handheld computer. This is because at ¶¶ [0015]-[0016] the database architecture supports *creating* software applications on a host computer/PC and hot-synching or IR beaming the created applications/content to the PDA/handheld computer where it is only *viewed and read*. See also ¶ [0064]. This PC/PDA divide runs through the entire Steele disclosure; see ¶¶ [0019]-[0027] for the proposition that at least Figs 2-8B relate to the PDA at which content is only read and displayed and at least Figs 9A-20 relate to the PC where content is created and edited.

Steele describes leaf nodes/pages which are asserted against the data assemblages of claim 20. Steele details at ¶ [0065] storing information as a hierarchy of nodes, in which the ending node references leafs which contains closely related information such as (in textual format) title, facts, Q & A, illustrations, and links to other leaf nodes in the database. These leafs or text files beamed to the PDA are asserted against the claimed data assemblages.

At ¶ [0067] Steele's database architecture provides password protection for specific leaf nodes. This password in Steele's imakerTM application is cited against the claimed security mechanism

Steele's leaf flag at ¶¶ [0076] & [0079] has two bits to indicate if the leaf has been visited at least once. We've termed this bit a "Seen flag", which is asserted against the claimed data attribute.

The clearest distinction lies in element d), keeping in mind that element c) *automatically* changes the data attribute *responsive to displaying* the SMS/data assemblage *for the first time*.

Security mechanism: First, para [0120] and also ¶¶ [0112]-[0113] and [0121] (which also detail the password function) show the password is enabled and set on the Steele PC, not the PDA/smartphone. ¶¶ [0112-0113] explicitly reference Figures 9A-10, and ¶ [0028] explicitly states that Figure 9A is at the PC. Second, ¶ [0120] explicitly states that the password protection is strictly for the edit function while the content/application is being created (see ¶¶ [0120]-[0123]). Since Steele does NO updating of the database at the PDA/smartphone per ¶ [0015], the password teachings are not seen to be relevant to either edit or display at the PDA/smartphone.

The final office action at page 15 discounts this by asserting that at ¶ [0115] Steele's imaker™ application also runs on the PDA. This implicitly assumes that the PC version of Steele's imaker™ is identical to the PDA version. ¶ [0115] explicitly negates that assumption: "The Re-edit option does not affect the performance of nor show up in any way on the application running on the handheld." There is no disclosure or teaching that editing may be done at the PDA, and the Steele password is activated only in the editing function. ¶ [0120] explicitly states that the edit function is only on the PC for creating content. Consistent with Steele's purpose at ¶ [0014] of avoiding the need to update records on the PDA, Steele's database architecture at ¶¶ [0015]-[0016] supports *creating* software applications on a host computer/PC. Thus the password of Steele is activated and set only at the PC, for the editing function.

¶ [0113] does disclose that the password is globally applied, and when it is activated one must enter it at the PDA to view the page. But this password is not activated in response to 1st display of the page at the PDA, it is manually activated and set according to an option provided to the user at the display screen of the PC as explicitly stated at ¶ [0012]. ¶ [0013] cited at page 15 of the final office action explicitly refers back to ¶ [0012]. There is no relation seen between the Steele password and Seen flag; when the password is activated at the PC it applies globally and is needed to view a page at the PDA, whether that viewing is the 1st display or the 50th display.

The final office action at page 16 asserts that Fig. 10 of Steele shows entering a password at the PDA/smartphone. The undersigned can find no text in Steele that characterizes Fig. 10 as a screenshot of the handheld. The header of that screenshot states: “Settings for Palm Application”, which can read on either the handheld or the PC. Because the explicit text of Steele cited in the above paragraph states that the password is activated in the edit function, and Steele creates/edits text ONLY at the PC, then consistency compels one of ordinary skill to see Fig. 10 of Steele as a screenshot of the PC, not the handheld.

The rejection asserts at page 5 that “Open import file” at ¶[0120] describes opening a text file without regard to password. This is commanded by “Ctrl+I” at ¶[0120] and Fig. 14, and so must refer to a full QWERTY keyboard at the PC, not Steele’s PDA. ¶ 0120] also describes “Export to Palm Format (Ctrl+E)” which exports to the PDA, and so both commands must be at the PC.

Seen flag: The interrelation between claim elements c) and d) require that for the rejection to be sustained there must be a relation between Steele’s Seen flag and Steele’s password. None is seen. Claim element d) recites restricting *further display*. Steele’s password is wholly irrelevant to how many times a page was displayed. Against this contention the final office action asserts at page 16 several propositions, summarized below and addressed seriatim.

Proposition 1: once a Steele file is saved and closed the page is password protected for editing.

Response 1: This is true for all pages for which the password function is activated, but holds regardless of 1st or 2nd display at the PC or PDA, and so regardless of the Steele’s Seen flag.

Proposition 2: ¶ [0077] describe a hidden attribute where a user chooses to hide a record, and ¶ [0079] suggests this would set the Seen flag.

Response 2: That the Steele user can choose to hide a record based on the Seen flag merely hides the record, it does not password protect it. This proposition is irrelevant to the password being activated for the hidden record. The next sentence of the final office action then assumes the password is activated and needed to view the page again, but this proposition makes no link between Steele’s Seen flag and Steele’s password which is manually activated and set at the PC. There remains no change to Steele’s password activation based on Seen flag.


Proposition 3: Automating the password protection is obvious to provide a more secure system since at ¶ [0120] there is motivation to prevent another tampering user from editing pages.

Response 3: Automating Steele's password simply makes it a default mode rather than user activated, but still unconnected to the Seen flag. If the Seen flag is flipped when a newly created page is closed after first being created, and the password is automatically activated by default, then this activity lies wholly within the PC since the PDA cannot create or edit content. Further, such a modification could never meet element c) of claim 20 since the Seen flag would be flipped and the password activated prior to the time the created page could be sent to the PDA.

The final office action also rebuts previous assertions of non-obviousness, concluding that Steele's invention is capable of being performed on the PDA since at ¶ [0115] the imakerTM application is resident on the PDA so there must be sufficient resources; and it would not require substantial redesign to relate the Seen flag to the password. Against the first clause above it is repeated, as detailed above, that the PDA version of imakerTM is not identical to the PC version; Steele explicit pre-empts this at ¶ [0009] by noting extremely limited handheld resources; and putting the full imakerTM on the PDA undermines Steele's overarching architecture by which only viewing and reading are done at the handheld ¶¶ [0012]-[0014]. Against the second clause it is repeated that there is no teaching to relate the Seen flag to the password; they serve different functions in Steele and there is no suggestion to relate them; and further that such a modification would be impermissible hindsight whether or not substantial redesign of Steele were required.

Claim 20 is seen to be non-obvious over Steele, alone or in combination with any other reference of record. Independent claims 33, 46 and 60 distinguish in substance for the same reasons as claim 20. The Applicants respectfully request that all pending claims finally be passed to issue.

Respectfully submitted:


Jerry Stanton
Reg. No.: 46,008

Oct 2, 2008
Date

Customer No.: 29683
HARRINGTON & SMITH, PC
4 Research Drive
Shelton, CT 06484-6212

Telephone: (203) 925-9400, ext 12
Facsimile: (203) 944-0245

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

10.2.2008
Date

Jessica Lee
Name of Person Making Deposit